

DEPARTMENT OF DEFENSE

Classified Information

Nondisclosure Agreement (SF 312)

And

Verbal Attestation

Briefing Pamphlet

MAY 2000

**Prepared by the Security Directorate
Office of the Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)**



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000



Foreword

MAY 26 2000

This pamphlet provides guidance on the Standard Form (SF) 312, "Classified Information Nondisclosure Agreement" and supersedes DoD 5200.1-PH-1, "Classified Information Nondisclosure Agreement (SF 312) Briefing Pamphlet," dated March 1989. It also accommodates a Secretary of Defense policy memorandum subject: Personal Attestation Upon Granting of Security Access," dated February 5, 1999 requiring every individual who is granted a Top Secret clearance or is granted access to a specially-controlled access category or compartment to make a verbal attestation affirming their commitment to conform to the conditions and responsibilities imposed by law or regulation upon those granted such clearance or access.

This pamphlet is authorized by DoD Directive 5200.1, "DoD Information Security Program," dated December 13, 1996 and includes a brief discussion of the background and purpose of the SF 312; the text of pertinent legislative and executive authorities; a series of questions and answers on implementation of the SF 312; a sample indoctrination required by paragraph 2 of the SF 312; and guidance for the conduct of verbal attestations.

The guidance contained herein with respect to the SF 312 is derived from that promulgated by the Information Security Oversight Office (ISOO) in collaboration with this office.

This pamphlet should be available in the offices of those individuals, e.g., security managers, security education specialists, or supervisors who brief individuals about the protection of classified information and request execution of the SF 312. Moreover, all persons who are asked to execute the SF 312, or have executed it or its predecessors, the SF 189 or SF 189-A, should have the opportunity to receive or borrow a copy upon request.

For additional guidance, please contact your Security Manager, supervisor, or legal counsel within your organization.

Comments of those using this pamphlet are invited and may be submitted to the Director, Security, Office of the Deputy

Assistant Secretary of Defense (Security and Information Operations), 6000 Defense, The Pentagon, Washington, D.C. 20301-6000, telephone DSN 225-2686 or commercial (703) 695-2686.



Richard F. Williams, CPP
Director of Security

TABLE OF CONTENTS

	Page
Background and Purpose	4
Sample Introduction Briefing	5
Verbal Attestation	10
Legislative and Executive Authorities	11
Executive Order 12958	19
Questions and Answers	47
Sample 312 Form	57

Background and Purpose

As an employee of the Department of Defense or one of its contractors, licensees, or grantees who occupies a position which requires access to classified information, you have been the subject of a personnel security investigation. The purpose of this investigation was to determine your trustworthiness for access to classified information. When the investigation was completed, your employing or sponsoring department or agency granted you a security clearance based upon a favorable adjudication of the investigation results. By being granted a security clearance, you have met the first of three requirements necessary to have access to classified information.

The second requirement that you must fulfill is to sign an SF 312, "Classified Information Nondisclosure Agreement." The President established this requirement in a Directive that states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." The SF 312 is a contractual agreement between the United States Government, and you a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of (1) the trust that is placed in you by providing you access to classified information; (2) your responsibilities to protect that information from unauthorized disclosure; and (3) the consequences that may result from your failure to meet those responsibilities. Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of non-compliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for such a disclosure by initiating a civil or administrative action.

The third and final requirement for access to classified information is the "need-to-know," that is, you must have a need to know the information in order to perform your official duties. The holder of classified information to which you seek access is responsible for confirming your identity, your clearance, and your need-to-know." As a holder of classified information, you are responsible for making these same determinations with respect to any individual to whom you may disclose it.

As a cleared employee you should receive, according to paragraph No. 2 of the SF 312, a "security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom you contemplate disclosing this information have been approved for access to it." After you receive such a briefing, you should have a basic understanding of the following:

- What is classified information?
- How do you protect it?
- Who may have access to it?
- How does the classification system function?

The indoctrination briefing that follows may be used as a basic introduction to these points.

In case of access to Top Secret or specially controlled information, as a condition of access, you will also be asked to verbally attest to your understanding of, and willingness to comply with, the provisions of the SF 312. Specific guidance on attestation requirements and the attestation process is contained in a separate section of this pamphlet.

Sample Indoctrination Briefing

Background. Unauthorized disclosures of classified information threaten the security of our citizens. As a result, the President has directed that all persons authorized access to classified information shall be required to sign a nondisclosure agreement (NdA) as a condition of access. Therefore, those individuals who decline to sign an NdA shall be denied access to classified information, and appropriate action will be taken to revoke the security clearances of those declining individuals who already have access to classified information.

Nondisclosure Agreements. The SF 312 is to be executed by all cleared Department of Defense (DoD) military and civilian personnel and contractor employees as a condition of access to classified information. Previously executed copies of the SF 189, "Classified Information Nondisclosure Agreement," and the SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" remain valid and will be interpreted and enforced in a manner that is fully consistent with the interpretation and enforcement of the SF 312. Therefore, any cleared individual who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312. However, at the individual's discretion, he or she may elect to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A.

Nature of Classified Information. Classified national security information (or classified information) is "information that has been determined pursuant to Executive Order (E.O.) 12958, "Classified National Security Information," April 17, 1995, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form." Information is classified under one of three designations, namely, "Top Secret," "Secret," or "Confidential," depending on the level of sensitivity.

"Top Secret" is applied only to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the Original Classification Authority is able to identify or describe.

"Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the Original Classification Authority is able to identify or describe.

"Confidential" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the Original Classification Authority is able to identify or describe.

Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, compromise of national-level cryptographic systems, exposure of some intelligence sources or methods, and substantial disruption of the capability of the National Command Authority to function in times of peace or crisis. Examples of "serious damage" and "damage" to national security are progressively less calamitous.

Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

If there is significant doubt about the appropriate level of classification, it should be classified at the lower level.

Note that security classification cannot be used to "conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization, or Agency; restrain competition; or prevent or delay the release of information that does not require protection in the interest of national security."

The Classification of Information. Information may be classified in one to two ways: originally or derivatively.

Original classification is an initial determination by an original classification authority, who has been designated in writing, that information requires protection against unauthorized disclosure in the interest of national security. The original classification process includes both the determination of the need to protect the information and the placement of security markings to identify the information as classified.

In determining the need for classification, a two-step process must be satisfied. First, the information must fall within one or more of the following classification categories:

- Military plans, weapons, or operations;
- Foreign government information;
- Intelligence activities (including special activities), or intelligence sources or methods, or cryptology;
- Foreign relations or foreign activities of the United States, including confidential sources;
- Scientific, technological, or economic matters relating to the national security;
- United States Government programs for safeguarding nuclear materials or facilities; or
- Vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security.

Secondly, the original classifier must determine that unauthorized disclosure of the information reasonably could be expected to cause damage to the national security. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security. The original classifier therefore need not make a separate determination that these categories meet the damage criteria.

Derivative Classification. Derivative classification is just as its name implies--classification derived from another source. It is the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material in a manner that is consistent with the security markings of the source information.

Within the Department of Defense, all cleared personnel who generate or create material that should be derivatively classified are responsible for ensuring that derivative classification is accomplished. No specific delegation of authority is required by persons doing derivative classification. DoD officials who sign or approve derivatively classified documents have principal responsibility for the quality of their derivative classification.

Information is classified derivatively in one of two ways--through the use of a source document such as a

security classification guide or other source document such as a report or correspondence. Information extracted from a classified report or correspondence to be incorporated into a new document is derivatively classified or not classified in accordance with the classification markings shown in the source document. The overall and internal markings of the source document should supply adequate classification guidance. If the source document is a classification guide, the derivative classification markings on the new document will be as prescribed by the guide.

Marking of Classified Information. At a minimum, classified documents must indicate (1) the highest level of classification; (2) the Agency or office of origin; (3) the identity of the Original Classification Authority or source document, as appropriate; and (4) a date or event for declassification. Refer to DoD 5200.1-R for guidance when unable to establish a date or event. In addition, each portion (e.g., titles, paragraphs) of a classified document must be marked to show level of classification, or that it is unclassified. For further information on marking classified documents, contact your Security Manager for a copy of DoD Pamphlet 5200.1-PH, "DoD Guide to Marking Classified Documents," April 1997.

Challenges to Classification. If you, as a holder of classified information, have substantial reason to believe that the information has been classified improperly or unnecessarily, you are encouraged and expected to bring it to the attention of your supervisor, Security Manager and/or the classifier of the information to bring about any necessary correction. The fact that you, as a DoD civilian employee, contractor employee, or military member of the Armed Forces, has issued a challenge to classification will not in any way result in or serve as a basis for adverse personnel action against you.

Protection of Classified Information. As a custodian of classified information, you have a personal, moral, and legal responsibility at all times to protect classified information, whether oral or written, within your knowledge, possession, or control and for locking classified information in approved security containers or otherwise physically securing the information it is not in use or under the direct supervision of authorized persons. Further, you must follow procedures that ensure that unauthorized persons do not gain access to classified information.

For example, classified material must not be discussed on the telephone, read, or discussed in public places. Don't be fooled by telephone callers who drop names or otherwise try to impress you with "urgent needs." Private codes or "talking around" classified information doesn't really fool anyone and should be strictly avoided. Further, many leaks of classified information result from conversations or interviews. Be very cautious in dealings with persons not authorized to have access to classified information. Remember, leaks may be just as damaging to our national security as outright espionage.

Care During Working Hours. Classified documents removed from storage must be kept under constant surveillance and face down or covered when not in use. Cover sheets used shall be Standard Forms 703, 704, and 705 for Top Secret, Secret, and Confidential documents, respectively.

Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, working sheets, typewriter ribbons, working papers, floppy and hard disks, and other items containing classified information must be either destroyed immediately after they have served their purpose, or be given the same classification and secure handling as the classified information they contain.

Classified information may be processed by automated information systems, but only by those systems that have been approved for such use.

Avoid routine reproduction of classified material. Classified material that is reproduced is subject to the same controls as the original material.

Memorize safe combinations and computer passwords. Never write a combination down on anything that is not securely stored in an approved security container or other approved security equipment. Classified information is not personal property and may not be removed from an activity's working area without specific authorization. Upon transfer or separation, all classified information in your custody must be returned to your supervisor or Security Manager. Destroy all classified information that is no longer required for operational or record purposes. Storing unneeded classified information increases both cost and risk. Check with your Security Manager for approved methods of destruction.

End-of-Day Security Checks. A system of security checks must be implemented at the close of each working day to ensure that all classified information is secure. Standard Form 701, "Activity Security Checklist," provides a systematic means to make a thorough end-of-day security inspection of a particular work area and shall be used to record such inspection. An integral part of the security inspection system is the security of all approved vaults, containers, and other approved equipment used for the storage of classified material. Standard Form 702, "Security Container Check Sheet," provides a record of the names and times that persons have opened, closed and checked a particular container or vault. Standard Forms 701 and 702 must be annotated to reflect after-hours, weekend, and holiday activity.

Access. No person may have access to classified information unless that person has been determined to be trustworthy, and unless access is essential to the accomplishment of lawful and authorized Government purposes, that is, the person has the appropriate security clearance and a demonstrated need-to-know. The final responsibility for determining whether a person's official duties require possession of or access to any element or item of classified information, and whether that person has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient. The possessor of the information is in the best position to determine whether a prospective recipient is cleared and has a need-to-know the information.

No one has a right to have access to classified information by possessing a security clearance alone but no need-to-know; solely by virtue of rank or position; or mere possession of a badge. Don't assume anything. Check identity, clearance, need-to-know, and ability to properly protect (or store) the information before passing classified information to anyone. Strictly limit distribution of papers and other media containing classified information. When in doubt, do not route. Avoid routine dissemination of classified material.

Administrative Sanctions and Reporting Requirements. By failing to follow these rules and precautions, we expose ourselves to serious penalties if classified information is purposely or even negligently disclosed or compromised. Such penalties include but are not limited to a warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge, fine and imprisonment.

You must immediately report any actual or suspected unauthorized disclosure of classified information to your supervisor or Security Manager, applicable Military Service investigative or counterintelligence organization, or to the FBI. Do not attempt to handle a security incident yourself--refer it to trained professionals.

Verbal Attestation

As previously indicated, all DoD military members and civilian employees who have been granted a Top Secret clearance or granted access to a specially controlled access category or compartment must make a verbal attestation. The verbal attestation must be witnessed by at least one individual in addition to the official who presides over the attestation and manages the process.

The procedures for personal attestation include:

Individual with Top Secret clearance or access to specially-controlled access category or compartments is to attest orally to the first paragraph of the SF 312. This verbal attestation must be made before an individual designated to preside over the attestation and a witness.

The presiding official will ensure the statement, "Attestation completed on (date)," is placed in the bottom of the Organization block in Item 11 of the SF 312.

The individual making the verbal attestation will complete Item 11 of the SF 312. The witness will sign in the Witness block. The Presiding official will sign in the Acceptance block.

The original of the SF 312 will be forwarded for retention in the attesting individual's personnel security file.

Legislative and Executive Authorities

Title 18, United States Code

§641. Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted--

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of \$100, he shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

§793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever, having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer--

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

§794. Gathering or delivering defense information to aid foreign government

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or

to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

§798. Disclosure of classified information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information--

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes--

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section--

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

§952. Diplomatic codes and correspondence

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code, or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

Title 50, United States Code

§952. Offenses

(b) Communication of classified information by Government officer or employee

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

TITLE VI -PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION¹

PROTECTION OF IDENTITIES OF CERTAIN UNITED STATES UNDERCOVER INTELLIGENCE OFFICERS, AGENTS, INFORMANTS, AND SOURCES

Sec. 601.(a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than \$50,000 or imprisoned not more than ten years, or both.

(b) Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than \$25,000 or imprisoned not more than five years, or both.

(c) Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined not more than \$15,000 or imprisoned not more than three years, or both.

¹Title VI was added by the Intelligence Identities Protection Act of 1982 (Public Law 97-200).

DEFENSES AND EXCEPTIONS

602.(a) It is a defense to a prosecution under section 601 that before the commission of the offense with which the defendant is charged, the United States had publicly acknowledged or revealed the intelligence relationship to the United States of the individual the disclosure of whose intelligence relationship to the United States is the basis for the prosecution.

(b) (1) Subject to paragraph (2), no person other than a person committing an offense under section 601 shall be subject to prosecution under such section by virtue of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

(2) Paragraph (1) shall not apply (A) in the case of a person who acted in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, or (B) in the case of a person who has authorized access to classified information.

(c) It shall not be an offense under section 601 to transmit information described in such section directly to the Select Committee on Intelligence of the Senate or to the Permanent Select Committee on Intelligence of the House of Representatives.

(d) It shall not be an offense under section 601 for an individual to disclose information that solely identifies himself as a covert agent.

Sec. 603.(a) The President, after receiving information from the Director of Central Intelligence, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives an annual report on measures to protect the identities of covert agents, and on any other matter relevant to the protection of the identities of covert agents.

(b) The report described in subsection (a) shall be exempt from any requirement for publication or disclosure. The first such report shall be submitted no later than February 1, 1983.

EXTRATERRITORIAL JURISDICTION

Sec. 604. There is jurisdiction over an offense under section 601 committed outside the United States if the individual committing the offense is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act).

PROVIDING INFORMATION TO CONGRESS

Sec. 605. Nothing in this title may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.

DEFINITIONS

For the purposes of this title:

(1) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term "authorized," when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means--

(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency--

(i) whose identity as such an officer, employee, or member is classified information, and

(ii) who is serving outside the United States or has within the last five years served outside the United States; or

(B) a United States citizen whose intelligence relationship to the United States is classified information, and--

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term "intelligence agency" means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by sections 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard.

EXECUTIVE ORDER #12958

CLASSIFIED NATIONAL SECURITY INFORMATION

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1 ORIGINAL CLASSIFICATION

Section 1.1. Definitions. For purposes of this order:

- (a) "National security" means the national defense or foreign relations of the United States.
- (b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.
- (c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- (d) "Foreign Government Information" means:
 - (1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
 - (2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
 - (3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6 c. of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Sec. 1.2. Classification Standards

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
 - (2) create any substantive or procedural rights subject to judicial review.
- (c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3. Classification Levels.

- (a) Information may be classified at one of the following three levels:
- (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
 - (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
 - (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
- (b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.
- (c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sect. 1.4. Classification Authority.

- (a) The authority to classify information originally may be exercised only by:
- (1) the President;
 - (2) agency heads and officials designated by the President in the Federal Register; or
 - (3) United States Government officials delegated this authority pursuant to paragraph (c), below.
- (b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.
- (c) Delegation of original classification authority.
- (1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5. Classification Categories. Information may not be considered for classification unless it concerns:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities; or vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. Duration of Classification.

(a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

- (1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;
- (2) reveal information that would assist in the development or use of weapons of mass destruction;
- (3) reveal information that would impair the development or use of technology within a United States weapons system;
- (4) reveal United States military plans, or national security emergency preparedness plans;
- (5) reveal foreign government information;
- (6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;
- (7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
- (8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7. Identification and Markings.

(a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

- (1) one of the three classification levels defined in section 1.3 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or

(C) the exemption category from classification, as prescribed in section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. Classification Prohibitions and Limitations.

(a) In no case shall information be classified in order to:

- (1) conceal violations of law, inefficiency, or administrative error;
- (2) prevent embarrassment to a person, organization, or agency;
- (3) restrain competition; or
- (4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

- (1) meets the standards for classification under this order; and
- (2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. Classification Challenges.

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

- (1) individuals are not subject to retribution for bringing such actions;
- (2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART 2 DERIVATIVE CLASSIFICATION

Sec. 2.1. Definitions. For purposes of this order:

(a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

Sec. 2.2. Use of Derivative Classification.

(a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. Classification Guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the

proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3 DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. Definitions. For purposes of this order:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in the records that have been determined by the Archivist of the United States

("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that maybe declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. General Responsibilities.

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
- (2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. Transferred Information.

(a) In case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor

agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4. Automatic Declassification.

(a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

- (5) reveal actual U.S. military war plans that remain in effect;
- (6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
- (7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
- (8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or
- (9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the file series;
- (2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the information;
- (2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the

President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5. Systematic Declassification Review.

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified information:

(1) accessioned into the National Archives as of the effective date of this order;

(2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and

(3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that

agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.6. Mandatory Declassification Review.

(a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for

administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. Declassification Database.

(a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART 4 SAFEGUARDING

Sec. 4.1. Definitions. For purposes of this order:

(a) "Access" means the ability or opportunity to gain knowledge of classified information.

(b) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. General Restrictions on Access.

(a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. Distribution Controls.

(a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. Special Access Programs.

(a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) Requirements and Limitations.

(1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6c of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. Access by Historical Researchers and Former Presidential Appointees.

(a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART 5 IMPLEMENTATION AND REVIEW

Sec. 5.1. Definitions. For purposes of this order:

(a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

Sec. 5.2. Program Direction.

(a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

- (1) classification and marking principles;
- (2) agency security education and training programs;
- (3) agency self-inspection programs; and
- (4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential

directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Sec. 5.3. Information Security Oversight Office.

(a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

- (1) develop directives for the implementation of this order;
- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;
- (4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;
- (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
- (7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
- (8) report at least annually to the President on the implementation of this order; and
- (9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4. Interagency Security Classification Appeals Panel.

(a) Establishment and Administration.

- (1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The

Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) Rules and Procedures. The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the federal courts; and

(3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President

through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Sec. 5.5. Information Security Policy Advisory Council.

(a) Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

(b) Functions. The Council shall:

(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) Meetings. The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) Administration.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the

Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. General Responsibilities. Heads of agencies that originate or handle classified information shall:

- (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;
- (b) commit necessary resources to the effective implementation of the program established under this order; and
- (c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:
 - (1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;
 - (2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;
 - (3) establishing and maintaining security education and training programs;
 - (4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;
 - (5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;
 - (6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;
 - (7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;
 - (8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) ensigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

PART 6 GENERAL PROVISIONS

Sec. 6.1. General Provisions.

(a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and

"Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. Effective Date.

This order shall become effective 180 days from the date of this order.

WILLIAM J. CLINTON

**THE WHITE HOUSE,
April 17, 1995.**

Implementing Rule of the "Classified Information Nondisclosure Agreement "Section 2003.20 of Title 32, Code of Federal Regulations as published in Vol. 53, *Federal Register*, p. 38278 September 29, 1988

32 CFR Part 2003 is amended as follows:

PART 2003 -- NATIONAL SECURITY INFORMATION - STANDARD FORMS

1. The authority citation for 32 CFR Part 2003 continues to read:

Authority: Sec. 5.2(b)(7) of E.O. 12356 (now E.O. 12958).

Subpart B - Prescribed Forms

2. Section 2003.20 is revised to read as follows:

§2003.20 Classified Information Nondisclosure Agreement: SF 312; Classified Information Nondisclosure Agreement: SF 189; Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government): SF 189-A

(a) SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual. The prior execution of at least one of these agreements, as appropriate, by an individual is necessary before the United States Government may grant that individual access to classified information. From the effective date of this rule, the SF 312 shall be used in lieu of both the SF 189 and the SF 189-A for this purpose. In any instance in which the language in the SF 312 differs from the language in either the SF 189 or the SF 189-A, agency heads shall interpret and enforce the SF 189 or SF 189-A in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

(b) All employees of executive branch departments, and independent agencies or offices, who have not previously signed the SF 189, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(c) All Government contractor, licensee, and grantee employees, or other non-Government personnel requiring access to classified information in the performance of their duties, who have not previously signed either the SF 189 or SF 189-A, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies, with cooperation of the pertinent contractor, licensee or grantee, shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(d) Agencies may require other persons, who are not included under paragraphs (b) or (c) of this section, and who have not previously signed either the SF 189 or SF 189-A, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies, with cooperation of the pertinent contractor, licensee or grantee, shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(e) The use of the "Security Debriefing Acknowledgement" portion of the SF 312 is optional at the discretion of the implementing agency.

(f) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.

(g) The provisions of the SF 312, the SF 189, and the SF 189-A do not supersede the provisions of Section 2302, United States Code, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(h) (1) *Modification of the SF 189.*

The second sentence of Paragraph 1 of every executed copy of the SF 189 is clarified to read:

As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, (now E.O. 12958) or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 (c) and 1.2 (e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security.

(2) *Scope of "classified information."*

As used in the SF 312, the SF 189, and the SF 189-A "classified information" is marked or unmarked classified information, including oral communications; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 (c) and 1.2 (e) of Executive Order 12356, or under any other Executive order or statute that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination.

(3) *Basis for liability.*

A party to the SF 312, SF 189 or SF 189-A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that: (i) the marked or unmarked information is classified, or meets the standards for classification and is in the process of a classification determination; and (ii) his or her action will result, or reasonably could result in the unauthorized disclosure of that information. In no instance may a party to the SF 312, SF 189 or SF 189-A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

(i) *Points of clarification.*

(1) As used in Paragraph 3 of SF 189 and SF 189-A, the word "indirect" refers to any situation in which the knowing, willful or negligent action of a party to the agreement results in the unauthorized disclosure of classified information even though the party to the agreement does not directly communicate, deliver or transmit classified information to a person who is not authorized to receive it.

(2) As used in Paragraph 7 of SF 189, "information" refers to "classified information," exclusively.

(3) As used in the third sentence of Paragraph 7 of SF 189 and SF 189-A, the words "all materials which have, or may have, come into my possession," refer to "all classified materials which have or may come into my possession," exclusively.

(j) Each agency must retain its executed copies of the SF 312, SF 189, and SF 189-A in file systems from which the agreements can be expeditiously retrieved in the event that the United States must seek their enforcement. The copies or legally enforceable facsimiles of them must be retained for 50 years following their date of execution. An agency may permit its contractors, licensees and grantees to retain the executed agreements of their employees during the time of employment. Upon the termination of employment, the contractor, licensee or grantee shall deliver the SF 312, SF 189, or SF 189-A of that employee to the Government agency primarily responsible for his or her classified work.

(k) Only the National Security Council may grant an agency's request for a waiver from the use of the SF 312. To apply for a waiver, an agency must submit its proposed alternative disclosure agreement to the Director of the ISOO, along with a justification for its use. The Director of ISOO will request a determination about the alternative agreement's enforceability from the Department of Justice prior to making a recommendation to the National Security Council. An agency that has previously received a waiver from the use of the SF 189 or SF 189-A need not seek a waiver from the use of the SF 312.

(l) The National Stock Number for the SF 312 is 7540-01-280-5499.

Questions and Answers

List of Questions

Question 1:	What is the Information Security Oversight Office?	49
Question 2:	What is the purpose of the SF 312?	49
Question 3:	Upon what legal authority is the SF 312 based?	49
Question 4:	Who must sign the SF 312?	49
Question 5:	Are all Members of Congress entitled to unlimited access to classified information?	50
Question 6:	Is an employee who signed an SF 312, SF 189 or SF 189-A in a prior position required to sign an SF 312 in a new position that also involves access to classified information?	50
Question 7:	Should a person who does not now have a security clearance but who may very well have such a clearance in the future sign the SF 312?	50
Question 8:	Should a person who has a security clearance but has no occasion to have access to classified information be required to sign the SF 312?	51
Question 9:	Must an employee execute the SF 312 at the time he or she is briefed about the requirement to do so?	51
Question 10:	What happens if a person who has not signed either the SF 189 or SF 189-A refuses to sign the SF 312?	51
Question 11:	How does the SF 312 differ from the SF 189 and SF 189-A?	52
Question 12:	For purposes of the SF 312, what is "classified information"?	52
Question 13:	What is the threshold of liability for violating the nondisclosure provisions of the SF 312?	52
Question 14:	May the language of the SF 312 be altered to suit the preferences of an individual signer?	53
Question 15:	Why are there separate entries on the SF 312 for the person who witnesses its execution by the employee and the person who accepts the agreement on behalf of the Government? Must different persons perform each function?	53

Question 16:	Does the SF 312 conflict with the "whistleblower" statute?	53
Question 17:	Must a signatory to the SF 312 submit any materials that he or she contemplates publishing for prepublication review by the employing or former employing agency?	54
Question 18:	Why do the obligations to protect classified information under the SF 312 extend beyond duration of an employee's clearance?	54
Question 19:	If information that a signer of the SF 312 knows to have been classified appears in a public source, for example, in a newspaper article, may the signer assume that the information has been declassified and disseminate it elsewhere?	54
Question 20:	What civil and administrative actions may the Government take to enforce the SF 312?	55
Question 21:	How long must executed copies of the SF 312 be retained? Where must they be stored? Can they be retained in a form other than the original papercopy?	55
Question 22:	May the signer keep a copy of the executed SF 312?	56
Question 23:	Does the verbal attestation apply to Department of Defense contractors?	56

Question 1: What is the Information Security Overnight Office?

Answer: Under Executive Order 12356, "National Security Information," the Information Security Oversight Office (ISOO) is responsible for monitoring the Information Security programs of all executive branch departments and agencies that create or handle national security information. In National Security Decision Directive No. 84, March 11, 1983, the President directed ISOO to develop and issue a standardized classified information nondisclosure agreement to be executed by all cleared persons as a condition of access to classified information.

Question 2: What is the purpose of the SF 312?

Answer: The primary purpose of the SF 312 is to inform employees of (a) the trust that is placed in them by providing them access to classified information; (b) their responsibilities to protect that information from unauthorized disclosure; and (c) the consequences that may result from their failure to meet those responsibilities. Secondly, by establishing the nature of that trust, those responsibilities and those consequences in the context of a contractual agreement, if that trust is violated, the United States will be in a better position to prevent an unauthorized disclosure or to discipline an employee responsible for such a disclosure by initiating a civil or administrative action.

Question 3: Upon what legal authority is the SF 312 based?

Answer: The direct legal bases for the issuance of SF 312 are Executive Order 12356, in which the President authorizes the Director of ISOO to issue standardized security forms; and National Security Decision Directive No. 84 (NSDD 84), in which the President directs ISOO to issue a standardized classified information nondisclosure agreement. Both E.O. 12356 and NSDD 84 are based on the President's constitutional responsibilities to protect national security information. These responsibilities derive from the President's powers as Chief Executive, Commander-in-Chief, and the principal architect of United States foreign policy.

Nondisclosure agreements have consistently been upheld by the Federal courts, including the Supreme Court, as legally binding and constitutional. At every stage of the development and implementation of the SF 312 and its predecessors, the SF 189 and the SF 189-A, experts in the Department of Justice have reviewed their constitutionality and enforceability under existing law. The most recent litigation over the SF 189 resulted in a decision that upheld its basic constitutionality and legality.

Question 4: Who must sign the SF 312?

Answer: As provided in National Security Decision Directive No. 84, dated March 11, 1983: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." Therefore, each person at the time that he or she is cleared for access to classified information, or each person who has been cleared previously and continues to require access to classified information must sign the SF 312, unless he or she has previously executed one or more of the following:

- (a) The SF 189, for cleared employees in both Government and industry;
- (b) The SF 189-A, for cleared employees within industry; or

(c) A nondisclosure agreement for which the National Security Council has granted a waiver from the use of the SF 312, the SF 189 or the SF 189-A, as provided in 32 CFR §2003.20.

By tradition and practice, United States officials who hold positions prescribed by the Constitution of the United States are deemed to meet the standards of trustworthiness for eligibility for access to classified information. Therefore, the President, the Vice President, Members of Congress, Supreme Court Justices, and other federal judges appointed by the President and confirmed by the Senate need not execute the SF 312 as a condition of access to classified information.

Question 5: Are all Members of Congress entitled to unlimited access to classified information?

Answer: No. Access to classified information is a function of three preconditions: (1) A determination of a person's trustworthiness, i.e., the security clearance; (2) the signing of an approved nondisclosure agreement; and (3) the exercise of the "need-to-know" principle, i.e., access is necessary in order to perform one's job. Members of Congress, as constitutionally elected officials, are not ordinarily subject to clearance investigations nor does ISOO's rule implementing the SF 312 require that Members of Congress sign the SF 312 as a condition of access to classified information. Members of Congress are not exempt, however, from fulfilling the "need-to-know" requirement. They are not inherently authorized to receive all classified information, but agencies provide access as is necessary for Congress to perform its legislative functions, for example, to members of a committee or Subcommittee that oversees classified executive branch programs. Frequently, access is governed in these situations by ad hoc agreements or rules to which the agency head and the committee chairman agree.

The three basic requirements for access to classified information mentioned in the opening paragraph apply to congressional staffs as well as executive branch employees. ISOO's regulation implementing the SF 312 provides that agency heads may use it as a nondisclosure agreement to be signed by non-executive branch personnel, such as congressional staff members. However, agency heads are free to substitute other agreements for this purpose.

Question 6: Is an employee who signed an SF 312, SF 189 or SF 189-A in a prior position required to sign an SF 312 in a new position that also involves access to classified information?

Answer: The SF 312 and its predecessors have been purposely designed so that new nondisclosure agreements need not be signed upon changing jobs. Therefore, ordinarily the answer is no. However, if the location and retrieval of a previously signed agreement cannot be accomplished in a reasonable amount of time or with a reasonable amount of effort, the execution of the SF 312 may be practicable or even necessary. Also, a person who has signed the SF 189-A, which was designed exclusively for non-Government employees, would be required to sign the SF 312 if he or she began working for a Government Agency in a position that required access to classified information.

Question 7: Should a person who does not now have a security clearance but who may very well have such a clearance in the future sign the SF 312?

Answer: No. The SF 312 should be signed only by persons who already have a security clearance or are being granted a security clearance at that time. It is inappropriate to have any uncleared person sign the SF 312, even if that person may have a need to be cleared in the near future.

Question 8: Should a person who has a security clearance but has no occasion to have access to classified information be required to sign the SF 312?

Answer: Since every cleared person must sign a nondisclosure agreement, the routine answer to this question is "yes." However, there are employees who have questioned executing a nondisclosure agreement on the basis that they have not had access to classified information over a lengthy period of time. Persons who do not require access to classified information should not have or retain security clearances. Therefore, the agency or contractor in such a situation should first determine the need for the retention of the security clearance. If its retention is unnecessary or speculative, the clearance should be withdrawn through established procedures and the employee should not sign the SF 312. If the agency or contractor determines a legitimate, contemporaneous need for the employee's clearance, the employee must sign the SF 312.

Question 9: Must an employee execute the SF 312 at the time he or she is briefed about the requirement to do so?

Answer: No. An employee who requests additional time to consider his or her decision to execute the SF 312 should be provided a reasonable amount of time to do so. The particular circumstances of the situation must govern what is a reasonable amount of time. In every situation, however, the agency or contractor should give the employee a written determination of the additional time that he or she shall have to make that decision. Also, in any situation in which there is a delay in the execution of the SF 312, the employee should be advised of the criminal, civil or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not yet signed the nondisclosure agreement.

Question 10: What happens if a person who has not signed either the SF 189 or SF 189-A refuses to sign the SF 312?

Answer: As provided by presidential directive, the execution of an approved nondisclosure agreement shall be a condition of access to classified information. Therefore, an agency shall take those steps that are necessary to deny a person who has not executed an approved nondisclosure agreement any further access to classified information. In accordance with agency regulations and procedures, the affected party's security clearance shall either be withdrawn or denied. For purposes of meeting this condition for access, the approved nondisclosure agreements include any of the following:

- (a) The SF 189, for cleared employees in both Government and industry,
- (b) The SF 189-A, for cleared employees within industry; or

A nondisclosure agreement for which the National Security Council has granted a waiver from the USC of the SF 312, the SF 189 or the SF 189-A, as provided in 32 CFR §2003.20.

While the refusal to sign a required nondisclosure agreement directly affects the withdrawal or denial of a security clearance, this, in turn, may also lead to adverse employment actions, including removal. The agency or contractor should advise each affected employee of the particular consequences that will or may result from his or her refusal to sign a required nondisclosure agreement.

Question 11: How does the SF 312 differ from the SF 189 and SF 189-A?

Answer: The most obvious difference between the SF 312 and the SF 189 or SF 189-A is that the SF 312 has been designed to be executed by both Government and non-Government employees. The SF 312 differs from the SF 189 and SF 189-A in several other ways as well.

First, the term "classifiable information," which has now been removed from paragraph 1 of the SF 189 by regulation, does not appear in the SF 312.

Second, the modifiers "direct" and "indirect," which appear in paragraph 3 of both the SF 189 and SF 189-A, do not appear in the new nondisclosure agreement.

Third, the "Security Debriefing Acknowledgement," which appears in the SF 189-A, but not the SF 189, is included in the SF 312. Its use is optional at the discretion of the implementing agency.

Fourth, the SF 312 includes specific references to marked or unmarked classified information and information that is in the process of a classification determination. These references have now been added to the SF 189 by regulation.

Fifth, the SF 312 specifically references a person's responsibility in situations of uncertainty to confirm the classification status of information before disclosure.

The SF 312 also contains several other editorial changes which clarify perceived ambiguities in the predecessor forms. Notwithstanding these changes, the SF 312 does not in any way differ from the SF 189 and SF 189-A with respect to the substance of the classified information that each has been designed to protect.

Question 12: For purposes of the SF 312, what is "classified information?"

Answer: As used in the SF 312, the SF 189, and the SF 189-A, "classified information" is marked or unmarked classified information, including oral communications; and unclassified information that meets the standards for classification and is in the process of a classification determination, as provided in Sections 1.1 (c) of Executive Order 12958 or under any other Executive order or statute that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination.

The current Executive order and statute under which "classified information," as used in the SF 312, is generated are Executive Order 12958, "Classified National Security Information," and the Atomic Energy Act of 1954, as amended.

Question 13. What is the threshold of liability for violating the nondisclosure provisions of the SF 312?

Answer: A party to the SF 312, SF 189 or SF 189-A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that: (a) the information is marked or unmarked information is classified, or meets the standards for classification and is in the process of a

classification determination; and (b) his or her action will result, or reasonably could result, in the unauthorized disclosure of that information. In no instance may a party to the SF 312, SF 189 or SF 189-A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

Question 14: May the language of the SF 312 be altered to suit the preferences of an individual signer?

Answer: No. The SF 312 as drafted has been approved by the National Security Council as meeting the requirements of NSDD 84, and by the Department of Justice as an enforceable instrument in a court of law. An agency may not accept an agreement in which the language has been unilaterally altered by the signer.

Question 15: Why are there separate entries on the SF 312 for the person who witnesses its execution by the employee and the person who accepts the agreement on behalf of the Government? Must different persons perform each function?

Answer: In most circumstances, one person may serve as both the witness and acceptor of the SF 312, and, in these cases, both entries should be affixed to the SF 312 at the time of execution. Different persons must perform each function only when a person authorized to witness the execution of the SF 312 in a particular situation is not authorized to accept it on behalf of the United States in that same situation. Then, the entry as witness should be affixed to the SF 312 at the time of execution, and the entry as acceptor should be affixed by an authorized person as soon as possible after execution.

Any executive branch employee may witness the execution of the SF 312 by a Government or non-Government employee.

An agency employee specifically authorized to do so may accept on behalf of the United States an SF 312 executed by either an employee of that same agency or a non-Government employee whose clearance is granted through that agency.

An authorized representative of a contractor, licensee, grantee, or other non-Government organization, designated to act as an agent of the United States, may witness and accept an SF 312 executed by an employee of that same organization.

Question 16: Does the SF 312 conflict with the "whistleblower" statute?

Answer: The SF 312 does not conflict with the "whistleblower" statute (5 U.S.C. §2302). The statute does not protect employees who disclose classified information without authority. If an employee knows or reasonably should know that information is classified, provisions of the "whistleblower statutes" should not protect that employee from the consequences of an unauthorized disclosure.

In addition, Executive Order 12958, Section 1.8(a) prohibits classification in order to "(1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) to prevent or delay the release of information that does not require protection in the interest of national security."

Finally, there are remedies available to whistleblowers that don't require the unauthorized disclosure of classified information. There are officials within the Government who are both authorized access to classified information and who are responsible for investigating instances of reported waste, fraud, and abuse. Further, each agency has designated officials to whom challenges to classification may be addressed or to whom a disclosure of classified information is authorized. For example, within the Department of Defense employees are encouraged and expected to challenge the classification of information that they believe is not properly classified. Special procedures have been established to expedite decisions on these challenges.

Question 17: Must a signatory to the SF 312 submit any materials that he or she contemplates publishing for prepublication review by the employing or former employing agency?

Answer: No. There is no explicit prepublication review requirement in the SF 312, as there is none in the SF 189 and SF 189-A. (**Note:** In accordance with DoD Manual 5105.21-M-1, "Sensitive Compartmented Information (SCI) Administrative Manual," "Prior to public disclosure in any form, an SCI-indoctrinated or debriefed individual will submit for security review all material intended for disclosure that may contain SCI or SCI-derived information." However, if an individual who has had access to classified information is concerned that something he or she has prepared for publication may contain classified information, that individual should be encouraged to submit it to his or her current or last employing agency for a voluntary review. In this way the individual will minimize the possibility of a subsequent action against him or her as a result of an unauthorized disclosure.

Question 18: Why do the obligations to protect classified information under the SF 312 extend beyond the duration of an employee's clearance?

Answer: The terms of the SF 312 specifically state that all obligations imposed on the signer "apply during the time the signer is granted access to classified information, and at all times thereafter." This provision recognizes that the duration of the national security sensitivity of classified information rarely has any relationship to the duration of any particular individual's clearance. The injury to the United States that may result from an unauthorized disclosure is not dependent on the current status of the discloser.

The obligations imposed by the SF 312 apply to classified information. If particular information has been declassified, under the terms of the SF 312, there is no continuing nondisclosure obligation on the part of the signer. Further, the signer of the SF 312 may initiate a mandatory review request to seek the declassification of specified classified information, including information to which the signer has access.

Question 19: If information that a signer of the SF 312 knows to have been classified appears in a public source, for example, in a newspaper article, may the signer assume that the information has been declassified and disseminate it elsewhere?

Answer: No. Information remains classified until it has been officially declassified. Its disclosure in a public source does not declassify the information. Of course, merely quoting the public source in the abstract is not a second unauthorized disclosure. However, before disseminating the information elsewhere or confirming the accuracy of what appears in the public source, the signer of the SF 312 must

confirm through an authorized official that the information has, in fact, been declassified. If it has not, further dissemination of the information or confirmation of its accuracy is also an unauthorized disclosure.

Question 20: What civil and administrative actions may the Government take to enforce the SF 312?

Answer: Among the civil actions that the Government may bring in Federal court are the application for a court order enjoining the publication or other disclosure of classified information; suits for money damages to recompense the United States for the damages caused by an unauthorized disclosure; and suits to require the forfeiture to the United States of any payments or other monetary or property gains that have resulted or may result from an unauthorized disclosure.

The scope of prospective administrative actions depends on whether the person alleged to have violated the SF 312 is a Government or non-Government employee. A Government employee would be subject to the entire range of administrative sanctions and penalties, including reprimand, suspension, demotion or removal, in addition to the likely loss of the security clearance.

In situations involving an unauthorized disclosure by a non-Government employee, the action will focus on the relationship between the Government and the organization that employs the individual. The Government cannot remove or otherwise discipline a non-Government employee, but it can, and in all likelihood will, revoke the security clearance of that employee, and prevent the employing organization from using that employee on classified projects. The Government may also move against the employing organization in accordance with the terms of their relationship. For example, in a Government contract situation, the Government may move to terminate the contract or to seek monetary damages from the contractor, based on the terms of the contract.

Although the enforcement of the SF 312, as a contractual instrument, is limited to civil or administrative actions, the Government may also criminally prosecute individuals or organizations that are alleged to have violated a criminal statute that involves the unauthorized disclosure of classified information. These criminal statutes are listed in the SF 312, and are reprinted in this Guide.

Question 21: How long must executed copies of the SF 312 be retained? Where must they be stored? Can they be retained in a form other than the original paper copy?

Answer: The originals or legally enforceable facsimiles of the SF 312 must be retained for 50 years following the date of execution. Ordinarily, microforms and other reproductions are legally enforceable in the absence of the originals. Each agency must retain its executed copies of SF 312 in a file system from which the agreement can be expeditiously retrieved in the event that the United States must seek their enforcement. Official personnel files, both for civilian and military service, ordinarily are not scheduled for preservation for a sufficient period of time to allow them to be used for this purpose.

The retention of the nondisclosure agreements by contractors shall be governed by instructions issued by the Defense Security Service or other agency that is responsible for security administration of the contractor's classified contracts. These instructions must take into account the retention and retrieval standards discussed above.

Question 22: May the signer keep a copy of the executed SF 312?

Answer: Ordinarily, a signer of the SF 312 who requests a copy of the executed form may keep one. Only in the extraordinary situation in which one of the signatures on the agreement reveals a classified relationship, resulting in the classification of that particular form, may the signer not keep a copy.

Question 23: Does the verbal attestation apply to Department of Defense contractors?

Answer: Yes. The Defense Federal Acquisition Regulation requires contractor employees granted a Top Secret clearance or access to a specially controlled access category or compartment to comply with the verbal attestation requirement.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN **AND THE UNITED STATES**

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.
10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)

Previous edition not usable.

STANDARD FORM 312 (REV. 1-91)
Prescribed by GSA/ISOO
32 CFR 2003, E.O. 12356

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)		

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (REV. 1-91)